AO 106 (Rev. 04/10) Application for a Search Warrant

United States District Court

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

iPhone seized from Yanyan Lesser at the Peace Bridge Port of Entry on February 22, 2019

Case No. 19-mj-36

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

iPhone seized from Yanyan Lesser at the Peace Bridge Port of Entry on February 22, 2019
See Attachment A

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B Items to be Searched for and Seized.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 USC 875(c) and 18 USC 373 *[statutory violation(s)]*.

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

CHARLES S. TOLIAS
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
Printed name and title

Sworn to before me and signed in my presence.

Date: March 5, 2019

Judge's signature

City and state: Buffalo, New York

HONORABLE H. KENNETH SCHROEDER, JR.
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, **CHARLES S. TOLIAS**, having been first duly sworn, do hereby depose and state as follows:

1. I am employed as a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), and have been employed in that capacity since December 2008. I am currently assigned to HSI, Buffalo, New York. Before that time, I was employed as a Customs and Border Protection Enforcement Officer for approximately six years. As a Special Agent, I am a federal law enforcement officer within the meaning of Rule 41(a) of the Federal Rules of Criminal Procedure, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses in violation of the United States Code.

2. I am conducting an investigation related to violation of the following statutes: 18 U.S.C. § 875 (c) (Interstate communication of threats); 18 U.S.C. § 373 (solicitation to commit a crime of violence), that is, stalking with the intent to seriously injure, in violation of 18 U.S.C. 2261A(a). I have probable cause to believe that evidence related to the above offenses is located on Yanyan LESSER's telephone, using phone number (716) 348-7008 (Subject Device) as more fully described and pictured in **Attachment A**.

3. Consequently, I am submitting this affidavit in support of a search warrant authorizing the search of the Subject Device. I am requesting authority to search the Subject Device, including Subscriber Identity Modules, or SIM cards, contained therein, for the items specified in **Attachment B**.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a search warrant authorizing the search of the aforementioned Subject Device for the items specified in **Attachment B** hereto, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the Subject Device, which was found in the possession of Yanyan LESSER on February 22, 2019, contain evidence relating to the commission of violations of 18 U.S.C. § 875 (c) (Interstate communication of threats) and 18 U.S.C. § 373 (solicitation to commit a crime of violence).

Summary of Relevant Technology

5. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "land line" telephones. A cellular telephone usually includes a "call log," which records the telephone number, date, and time of calls made to and from the phone.

6. In addition to enabling voice communications, cellular telephones offer a broad range of other capabilities. These capabilities include, but are not limited to: (a) storing names and phone numbers in electronic "address books"; (b) sending, receiving, and storing text messages and emails; (c) taking, sending, receiving, and storing still photographs and videos; (d) storing and playing back audio files; (e) storing dates, appointments, and other information on personal calendars; and (f) accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

7. A Subscriber Identity Module, more commonly referred to as a SIM card, is a removable memory chip that is used in some models of cellular telephones. The SIM card is capable of holding a variety of personal data including telephone numbers, text messages, images, and billing information. The SIM card can be moved from one cellular phone to another and will display the saved data on each compatible phone into which it is inserted.

Facts Supporting Probable Cause

8. On February 19, 2019, HSI St. Paul, Minnesota, received information that between February 14, 2019, and February 19, 2019, an unidentified subject utilizing the moniker "TREE1" conspired with an unknown subject on a dark web site named Website #1 to commit a crippling assault of a subject (G.Z.) residing in Orlando, Florida.[1] "TREE1"

1 The actual name of Website #1 is known to law enforcement. The site remains active and disclosure of the name of the site would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of ongoing investigations, specific names and other identifying factors have been replaced with generic terms.

directed what was believed to be a hitman found via Website #1 to break G.Z.'s bones and leave him permanently confined to a wheelchair or crutches.

9. On February 16, 2019, "TREE1" transferred approximately 1.26 Bitcoin (BTC) (approximately $4,577.51 USD) to a BTC wallet address in the control of WEBSITE #1 to facilitate the assault. On February 19, 2019, "TREE1" conducted an additional transfer of approximately .694 BTC (approximately $2,707.95 USD) to the same WEBSITE #1 wallet address to further the request. In addition to the BTC transfers, "TREE1" provided a photograph to WEBSITE #1 of an unknown individual's lower back area with the words "broken waist" written across it.

10. On February 20, 2019, HSI Orlando conducted an interview of G.Z. at his residence in Orlando, Florida. G.Z. stated that he was not aware of any threat against him, but stated that he believed that his ex-girlfriend, Yanyan CUI, residing in Buffalo, New York would be capable of doing something like this as she is unstable. G.Z. provided telephone number (716) 348-7008 for CUI. G.Z. stated that he terminated his relationship with CUI on February 10, 2019, and that he has not spoken to her since.

11. Law enforcement system checks show that CUI submitted a United States State Department K1 (fiancé) VISA Application in 2007. Paul Lesser was listed on the application. According to information provided to your affiant by Mr. Lesser, he and CUI married and have since divorced. It is your affiant's belief that CUI is currently utilizing her married name (LESSER).

12. On February 26, 2019, your affiant served a DHS Summons to Verizon Wireless for information associated to telephone number (716) 348-7008. On March 4, 2019, Verizon Wireless provided the following subscriber information associated to the telephone number:

a. Subscriber Name: Yanyan LESSER

b. Subscriber Address: 401 N Star Road, East Aurora, New York

c. Subscriber Status: Active

d. Subscriber Effective Date: 12/29/2014

e. Account Number: 288591735-1

f. IMEI: 357265097778847

13. On February 22, 2019, LESSER crossed at the Peace Bridge Port of Entry located in Buffalo, New York. LESSER was the driver and sole occupant of a vehicle bearing New York State license plate #HCA5197. LESSER stated to United States Customs and Border Protection (CBP) that she traveled to Chinatown located in Toronto, Ontario, Canada to eat and that she was in Canada for approximately forty minutes. LESSER further stated that she currently resides at 401 North Road, East Aurora, New York. LESSER said that she enjoys Canada and that it is relaxing to her as she recently broke up with her boyfriend and that she is also going through a divorce with her husband. CBP noted that LESSER was in possession of an Apple iPhone at the time of her crossing.

14. HSI Buffalo Special Agent (SA) Tolias responded to the Peace Bridge port of entry to conduct a preview of LESSER's iPhone. LESSER stated that the iPhone in her

possession belonged to her and that it was the only telephone that she owns. LESSER told SA Tolias and CBP that she would unlock her Apple iPhone, but that she would not provide her password. LESSER subsequently unlocked her iPhone.

15. A review of the home screen by SA Tolias revealed what appeared to be a TOR application as well as a VPN application. The TOR network is an anonymous network that can only be accessed with a special web browser, called the TOR browser. TOR stands for "The Onion Router," a reference to the many layers in an onion. This is the portion of the World Wide Web most widely known for illicit activities because of the anonymity associated with the TOR network. The vast majority of goods for sale on dark web Marketplaces consist of illegal drugs, of nearly every variety, openly advertised on the site and prominently visible. In addition to illegal drugs, dark web Marketplaces openly advertise child pornography, identity documents, firearms, hitman services, and other contraband or regulated products. Silk Road, Dream, Hansa, and AlphaBay are examples of dark web Marketplaces known to law enforcement that previously or currently market illicit goods and activities. WEBSITE #1 is only accessible utilizing TOR. Bitcoin is the most common and widely accepted form of payment for illicit activities on the dark web.

16. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections,

encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

17. SA Tolias also conducted a preview of photographs contained on LESSER's iPhone and saw what appeared to be the image of the unknown individual's lower back area with the words "broken waist" written across it (as previously detailed above in paragraph 5). SA Tolias noted that it appeared to be the same exact photograph of the unknown individuals lower back area, but that the photograph did not have the words "broken waist" written across it.

18. LESSER's iPhone screen subsequently locked shortly thereafter, and the contents on the phone were no longer viewable.

19. LESSER had several banking withdrawal receipts in her possession corresponding with the dates that "TREE1" conspired with the unknown subject on the dark web site WEBSITE #1 to commit the crippling assault of G.Z. (between February 14, 2019, and February 19, 2019). The following receipts were found in LESSER's possession:

2/15/2019

Bank of America withdrawal in the amount of $2600.00

2/16/2019

TD Bank withdrawal in the amount of $100.00

2/18/2019

Bank of America withdrawal in the amount of $400.00

2/18/2019

Bank of Akron transaction denied (too many wrong password attempts)

20. A review of chat correspondence between "TREE1" and the purported hitman from Website #1 revealed the following messages:

2/15/2019 Website #1 Admin:

Hi, Please google how to buy bitcoins and find the best site for you Local bitcoins is ok but you need to select a trader with a good exchange rate. Best regards Juan admin Website #1 cyberteam

2/15/2019 TREE1

Hi I just exchanging cash into btc with trader from btc site in person.how can I find a btc mixer that mixes all the incoming transactions to your site?

21. Based on your affiants training and experience, localbitcoins.com offers an individual a means to purchase BTC and other crypto currencies anonymously. One such way is to purchase BTC for cash via an in-person/face to face meeting. This method ensures

that an individual's identity remains untraceable as there is no documentation of the transaction.

Electronic Storage and Forensic Analysis

22. Based on my knowledge, training, and experience, your affiant knows that cellular telephones are common communication devices used by individuals engaged in dark web and/or illicit cryptocurrency transactions. Such individuals typically store in their cellular telephones the telephone numbers of co-conspirators, as well as text and data messages with their co-conspirators.

23. Based on my knowledge, training, and experience, your affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on electronic devices. This information can sometimes be recovered with forensics tools.

24. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how the Subject Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the electronic device and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant your affiant is applying for would permit the examination of the Subject Device consistent with the warrant. The examination may require authorities

to employ techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, your affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night

REQUEST FOR SEALING

27. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left with LESSER). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

28. Based upon the foregoing facts and information, I respectfully submit there is probable cause to believe that the items to be searched, described in **Attachment A**, found in the possession of LESSER on February 22, 2019, was used to facilitate the criminal activities alleged, and as such, contain evidence, as set forth in particular in **Attachment B**, relating to the commission of violations of Title 18 U.S.C. § 875 (c) (Interstate communication of threat) and Title 18 U.S.C. § 373 (solicitation to commit a crime of violence).

29. **WHEREFORE**, in consideration of the foregoing, it is respectfully requested that this Court issue the requested search warrant authorizing the search of each item, described in **Attachment A**, for the items described in **Attachment B**.

CHARLES S. TOLIAS
Special Agent
Homeland Security Investigations

Sworn to before me this

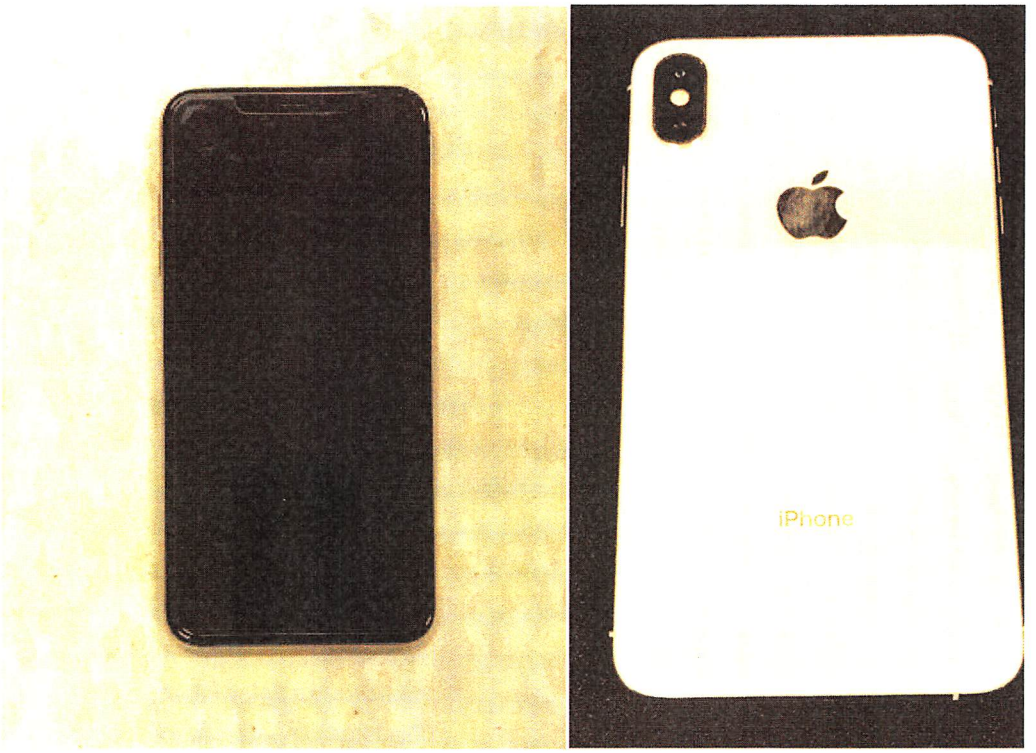
5th day of March , 2019.

H. KENNETH SCHROEDER, JR.
United States Magistrate Judge

ATTACHMENT A: SUBJECT DEVICE

Subject Device:

The property to be searched is a silver Apple iPhone XS Max assigned to telephone phone number (716) 348-7008, that belongs to Yanyan LESSER. The cellular telephone, which was in LESSER's possession when she was encountered on February 22, 2019, at the Peace Bridge Port of Entry is currently in possession of Homeland Security Investigations, 250 Delaware Avenue, Buffalo, New York.



ATTACHMENT B
Particular Things to be Searched for and Seized

All records and information on the Subject Device described in Attachment A that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 875 (c) (Interstate communications of threats) and 18 U.S.C. 373 (solicitation to commit a crime of interstate violence), that is stalking with the intent to seriously injure in violation of 18 U.S.C. 2261A(a) including but not limited to:

1. Content of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, social media account activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above;

2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of the times the devices were used;

4. Passwords, encryption keys, and other access devices that may be necessary to access the devices;

5. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violation described above.